WHAT IS CLAIMED IS:

Sub B1

1. A function randomness evaluating apparatus comprising at least one of:

higher-order-differential cryptanalysis resistance evaluating means for calculating the minimum value of the degree of a Boolean polynomial for input bits by which output bits of a function to be evaluated are expressed, and evaluating that the larger said minimum value, the higher the resistance of said function to higher order differential cryptanalysis is;

interpolation-cryptanalysis resistance evaluating means for: when fixing a key y and letting x denote the input of a function to be evaluated, expressing an output y by $y = f_k(x)$ using a polynomial over Galois field which is composed of elements equal to a prime p or a power of said prime p; calculating the number of terms of said polynomial; and evaluating the resistance of said function to interpolation cryptanalysis based on the result of said calculation;

partitioning-cryptanalysis resistance evaluating means for: dividing all inputs of a function to be evaluated and the corresponding outputs into input subsets and output subsets; calculating an imbalance of the relationship between the subset of an input and the subset of the corresponding output with respect to their average corresponding relationship; and evaluating the resistance of said function to partitioning cryptanalysis based on the result of said calculation; and

differential-linear-cryptanalysis resistance evaluating means for: calculating, for all sets of input difference Δx and output mask value Γy of a function S(x) to be evaluated, the number of inputs x for which the inner product of $(S(x)+S(x\Delta x))$ and said output mask value Γy is 1; and

evaluating the resistance of said function to differential-linear cryptanalysis based on the result of calculation.

2. The function randomness evaluating apparatus of claim 1, wherein:

said partitioning-cryptanalysis resistance evaluating means is means for: dividing an input set F and an output set G of said function into u input subsets $\{F_0, F_1, \ldots, {}_{Fu-1}\}$ and v output subsets $\{G_0, G_1, \ldots, G_{v-1}\}$; for each partition-pair (F_i, G_i) ($i = 0, \ldots, u-1$; $j = 0, 1, \ldots, v-1$), calculating the maximum one of probabilities that all outputs y corresponding to all inputs x of the input subset F_i belong to the respective output subsets G_j ($j = 0, \ldots, v-1$); calculating a measure $I_S(F, G)$ of an average imbalance of a partition-pair (F, G) based on all maximum values calculated for all partition pairs; and evaluating the resistance of said function to said partitioning cryptanalysis based on said measure; and

said differential-linear cryptanalysis resistance evaluating means is means for: calculating the following equation for every set of said input difference Δx except 0 and said output mask value Γy except 0

$$\xi_S(\Delta x, \Gamma y) = \left|2\times\#\{x \in GF(2)^n \mid (S(x) + S(x+\Delta x)) \bullet \Gamma y = 1\} - 2^n\right|;$$

calculating the maximum value Ξ among the calculation results; and evaluating the resistance of said function to said differential-linear cryptanalysis based on said value Ξ.

3. The function randomness evaluating apparatus of claim 1 or 2, further comprising at least one of:

differential-cryptanalysis resistance evaluating means for calculating, for a function S(x) to be evaluated, the number of inputs x that satisfy $S(x)+S(x+S(x+\Delta x)=\Delta y$ for every set $(\Delta x, \Delta y)$ and evaluating the

resistance of said function to differential cryptanalysis based on the result of said calculation; and

linear-cryptanalysis resistance evaluating means for calculating, for a function to be evaluated, the number of inputs x for which the inner product of the input x and its mask value Γx is equal to the inner product of a function output value S(x) and its mask value Γy and evaluating the resistance of said function to linear cryptanalysis based on the result of said calculation.

4. The randomness evaluating apparatus of claim 3, wherein said linear-cryptanalysis resistance evaluating means is means for calculating the following equation

$$\lambda_S(\Gamma x, \Gamma y) = \left| 2 \times \# \{ x \in (2)^n \mid x \bullet \Gamma x = S(x) \bullet \Gamma y \} - 2^n \right|$$

for every set of mask values (Γx, Γy) except $\Gamma y=0$, and evaluating the resistance of said function to said linear cryptanalysis based on a criterion defined by the following equation

$$\Lambda_S = \max \lambda_S(\Gamma x, \Gamma y).$$

5. The randomness evaluating apparatus of claim 3, wherein said differential-cryptanalysis resistance evaluating means is means for calculating the following equation

$$\delta_S(\Delta x, \Delta y) = \# \{ x \in GF(2)^n \mid S(x) + S(x + \Delta x) = \Delta y \}$$

for every set of difference values (Δx, Δy) except $\Delta x=0$, and evaluating the resistance of said function to said differential cryptanalysis based on a criterion defined by the following equation

$$\Delta_S = \max \delta_S(\Delta x, \Delta y).$$

6. A random function generating apparatus comprising:

candidate function generating means for generating candidate

functions each formed by a combination of a plurality of functions of different algebraic structures and having a plurality of parameters;

resistance evaluating means for evaluating the resistance of each of said candidate functions to a cryptanalysis; and

selecting means for selecting those of said resistance-evaluated candidate functions which have highly resistant to said cryptanalysis.

7. The random function generating apparatus of claim 6, wherein one of said plurality of functions of different algebraic structures is resistant to each of differential cryptanalysis and linear cryptanalysis.

8. The random function generating apparatus of claim 6 or 7, wherein said resistance evaluating means comprises at least one of:

higher-order-differential cryptanalysis resistance evaluating means for: calculating the minimum value of the degree of a Boolean polynomial for input bits by which output bits of each of said candidate functions are expressed; and evaluating the resistance of said each candidate function to higher order cryptanalysis based on the result of said calculation;

interpolation-cryptanalysis resistance evaluating means for: when fixing a key y and letting x denote the input of said each candidate, expressing an output y by $y = f_k(x)$ using a polynomial over Galois field which is composed of elements equal to a prime p or a power of said prime p; calculating the number of terms of said polynomial; and evaluating the resistance of said each candidate function to interpolation cryptanalysis based on the result of said calculation;

partitioning-cryptanalysis resistance evaluating means for: dividing all inputs of a function to be evaluated and the corresponding outputs into input subsets and output subsets; calculating an imbalance of the relationship between the subset of an input and the subset of the

corresponding output with respect to their average corresponding relationship; and evaluating the resistance of said function to partitioning cryptanalysis based on the result of said calculation; and

differential-linear cryptanalysis resistance evaluating means for: calculating, for every set of input difference Δx and output mask value Γy of a function S(x) to be evaluated, the number of inputs x for which the inner product of $(S(x)+S(x\Delta x))$ and said output mask value Γy is 1; and evaluating the resistance of said function to differential-linear cryptanalysis based on the result of said calculation.

9. A method for evaluating the randomness of the input/output relationship of a function, said method comprising at least one of:

(a) a higher-order-differential cryptanalysis resistance evaluating step of: letting said function be represented by S(x), calculating the minimum value of the degree of a Boolean polynomial for input bits of said function S(x) by which its output bits are expressed; and evaluating the resistance of said function to higher order cryptanalysis based on the result of said calculation;

(b) a differential-linear cryptanalysis resistance evaluating step of: calculating, for every set of input difference Δx and output mask value Γy of a function S(x) to be evaluated, the number of inputs x for which the inner product of $(S(x)+S(x\Delta x))$ and said output mask value Γy is 1; and evaluating the resistance of said function to differential-linear cryptanalysis based on the result of said calculation;

(c) a partitioning-cryptanalysis resistance evaluating step of: dividing all inputs of a function to be evaluated and the corresponding outputs into input subsets and output subsets; calculating an imbalance of the relationship between the subset of an input and the subset of the

corresponding output with respect to their average corresponding relationship; and evaluating the resistance of said function to partitioning cryptanalysis based on the result of said calculation; and

(d) an interpolation-cryptanalysis resistance evaluating step of: when fixing a key y and letting x denote the input of said each candidate, expressing an output y by y = $f_k(x)$ using a polynomial over Galois field which is composed of elements equal to a prime p or a power of said prime p; calculating the number of terms of said polynomial; and evaluating the resistance of said function to interpolation cryptanalysis.

10. The randomness evaluating method of claim 9, wherein:

said differential-linear cryptanalysis resistance evaluating step (b) is a step of:, letting the input difference and output mask value of said function S(x) be representing by Δx and Γy, respectively, calculating the following equation for every set of said input difference Δx except 0 and said output mask value Γy except 0

$$\xi_S(\Delta x, \Gamma y) = \left|2\times\#\{x\in GF(2)^n \middle| (S(x) + S(x+\Delta x)\bullet \Gamma y = 1\} - 2^n\right|;$$

calculating the maximum value Ξ among the calculation results; and evaluating the resistance of said function to said differential-linear cryptanalysis using said value Ξ; and

said partitioning-cryptanalysis resistance evaluating step (c) is a step of: dividing an input set F and an output set G of said function into u input subsets $\{F_0, F_1, \ldots, {}_{F_{u-1}}\}$ and v output subsets $\{G_0, G_1, \ldots, G_{v-1}\}$; for each partition-pair (F_i, G_i) (i = 0, ..., u-1; j = 0, 1, ..., v-1), calculating the maximum one of probabilities that all outputs y corresponding to all inputs x of the input subset F_i belong to the respective output subsets G_j (j = 0, ..., v-1); calculating a measure $I_S(F, G)$ of an average imbalance of a partition-pair

(F, G) based on all maximum values calculated for all partition pairs; and evaluating the resistance of said function to said partitioning cryptanalysis based on said measure.

11. The randomness evaluating method of claim 9 or 10, further comprising at least one of:

(e) a differential-cryptanalysis resistance evaluating step of: letting the output difference value of said function S(x) be represented by Δx, calculating the number of inputs x that satisfy $S(x)+S(x+S(x+\Delta x)=\Delta y$ for every set $(\Delta x, \Delta y)$ except $\Delta x=0$; and evaluating the resistance of said function to differential cryptanalysis based on the result of said calculation; and

(f) a linear-cryptanalysis resistance evaluating means for calculating, for said function S(x), the number of inputs x for which the inner product of the input x and its mask value Γx is equal to the inner product of a function output value S(x) and its mask value Γy and evaluating the resistance of said function to linear cryptanalysis based on the result of said calculation.

12. The randomness evaluating method of claim 11, wherein, letting the number of bits of said input x be represented by n:

said differential-cryptanalysis resistance evaluating step (e) is a step of: calculating the following equation

$$\delta_S(\Delta x, \Delta y) = \#\{x \in GF(2)^n \mid S(x) + S(x + \Delta x) = \Delta y\}$$

for every set of difference values $(\Delta x, \Delta y)$ except $\Delta x=0$; and evaluating the resistance of said function to said differential cryptanalysis based on a criterion defined by the following equation

$$\Delta_S = \max \delta_S(\Delta x, \Delta y);$$ and

said linear-cryptanalysis resistance evaluating step (f) is a step of: letting the mask value of said input x be represented by Γx, calculating the

following equation

$$\lambda_S(\Gamma x, \Gamma y) = \left|2 \times \#\{x \in (2)^n \,|\, x \bullet \Gamma x = S(x) \bullet \Gamma y\} - 2^n\right|$$

for every set of mask values (Γx, Γy) except Γy=0; and evaluating the resistance of said function to said linear cryptanalysis based on a criterion defined by the following equation

$$\Lambda_S = \max \lambda_S(\Gamma x, \Gamma y).$$

13. A random function generating method comprising the steps of:

(a) setting various values as each parameter for candidate functions and calculating output values corresponding to various input values;

(b) storing the results of said calculation in storage means; and

(c) evaluating the resistance of each of said candidate functions to a cryptanalysis based on values stored in said storage means, and selectively outputting candidate function highly resistant to said cryptanalysis; and

wherein said step (c) comprising at lease one of:

(c-1) a higher-order cryptanalysis resistance evaluating step of: calculating the minimum value of the degree of a Boolean polynomial for input bits of each of said candidate functions by which its output bits are expressed; evaluating the resistance of said each candidate function to higher order cryptanalysis based on the result of said calculation; and leaving those of said candidate functions whose resistance is higher than a predetermined first reference and discarding the others;

(c-2) a differential-linear cryptanalysis resistance evaluating step of: calculating, for every set of input difference Δx and output mask value Γy of each candidate function S(x), the number of inputs x for which the inner product of (S(x)+S(xΔx)) and said output mask value Γy is 1; evaluating the resistance of said function to differential-linear cryptanalysis based on

the result of said calculation; and leaving those of said candidate functions whose resistance is higher than a predetermined second reference and discarding the others;

(c-3) a partitioning-cryptanalysis resistance evaluating step of: dividing all inputs of each candidate function and the corresponding outputs into input subsets and output subsets; calculating an imbalance of the relationship between the subset of an input and the subset of the corresponding output with respect to their average corresponding relationship; evaluating the resistance of said each candidate function to said partitioning cryptanalysis based on the result of said calculation; and leaving those of said candidate functions whose resistance is higher than a predetermined third reference and discarding the others; and

(c-4) an interpolation-cryptanalysis resistance evaluating step of: when fixing a key y and letting x denote the input of said each candidate, expressing an output y by $y = f_k(x)$ using a polynomial over Galois field which is composed of elements equal to a prime p or a power of said prime p; calculating the number of terms of said polynomial; evaluating the resistance of said function to interpolation cryptanalysis; and leaving those of said candidate functions whose resistance is higher than a predetermined fourth reference and discarding the others.

14. The random function generating apparatus of claim 13, wherein:

said differential-linear-cryptanalysis resistance evaluating step (c-2) includes a step of: letting the output mask value be represented by Γy, calculating the following equation for every set of said input difference Δx except 0 and said output mask value Γy except 0

$$\xi_S(\Delta x, \Gamma y) = \left| 2 \times \#\{x \in GF(2)^n \,|\, (S(x) + S(x + \Delta x)) \bullet \Gamma y = 1\} - 2^n \right|;$$

calculating the maximum value Ξ among the calculation results; and evaluating the resistance of said candidate function to said differential-linear cryptanalysis based on said value Ξ; and

said partitioning0cryptanalysis resistance evaluating step (3) includes a step of dividing an input set F and an output set G of said function into u input subsets $\{F_0, F_1, \ldots, {}_{Fu-1}\}$ and v output subsets $\{G_0, G_1, \ldots, G_{v-1}\}$; for each partition-pair (F_i, G_i) ($i = 0, \ldots, u-1; j = 0, 1, \ldots, v-1$), calculating the maximum one of probabilities that all outputs y corresponding to all inputs x of the input subset F_i belong to the respective output subsets G_j ($j = 0, \ldots, v-1$); calculating a measure $I_S(F, G)$ of an average imbalance of a partition-pair (F, G) based on all maximum values calculated for all partition pairs; and evaluating the resistance of said candidate function to said partitioning cryptanalysis based on said measure.

15. The random function generating method of claim 13 or 14, wherein:

said step (c-1) includes a step of: when no candidate function remains undiscarded, easing the candidate function selecting condition by changing said first reference by a first predetermined width, and executing again the evaluation and selecting process;

said step (c-2) includes a step of: when no candidate function remains undiscarded, easing the candidate function selecting condition by changing said second reference by a second predetermined width, and executing again the evaluation and selecting process;

said step (c-3) includes a step of: when no candidate function remains undiscarded, easing the candidate function selecting condition by changing said third reference by a third predetermined width, and executing again the evaluation and selecting process; and

said step (c-4) includes a step of: when no candidate function remains undiscarded, easing the candidate function selecting condition by changing said fourth reference by a fourth predetermined width, and executing again the evaluation and selecting process.

16. The random function generating method of claim 13 or 14, further comprising at least one of:

(c-5) a differential-cryptanalysis resistance evaluating step of: calculating, for each candidate function S(x), the number of inputs x that satisfy S(x)+S(x+S(x+Δx)=Δy for every set (Δx, Δy) except Δx; evaluating the resistance of said each candidate function to differential cryptanalysis based on the result of said calculation; and leaving those of said candidate functions whose resistance is higher than a predetermined fifth reference and discarding the others; and

(c-6) a linear-cryptanalysis resistance evaluating step of: calculating, for each candidate function, the number of inputs x for which the inner product of the input x and its mask value Γx is equal to the inner product of a function output value S(x) and its mask value Γy; evaluating the resistance of said each candidate function to linear cryptanalysis based on the result of said calculation; and leaving those of said candidate functions whose resistance is higher than a predetermined sixth reference and discarding the others.

17. The random function generating method of claim 16, wherein:

said differential-cryptanalysis resistance evaluating step (c-5) includes a step of: calculating the following equation

$$\delta_S(\Delta x,\Delta y)=\#\{x\in GF(2)^n \,|S(x)+S(x+\Delta x)=\Delta y\}$$

for every set of difference values (Δx, Δy) except Γy=0; and evaluating the resistance of said each candidate function to said differential

cryptanalysis based on a criterion defined by the following equation

$$\Delta_S = \max \delta_S(\Delta x, \Delta y);$$ and

said linear-cryptanalysis resistance evaluating step (c-6) includes a step of: calculating the following equation

$$\lambda_S(\Gamma x, \Gamma y) = \left|2 \times \#\{x \in (2)^n \,|\, x \bullet \Gamma x = S(x) \bullet \Gamma y\} - 2^n\right|$$

for every set of mask values (Γx, Γy); and evaluating the resistance of said each candidate function to said linear cryptanalysis based on a criterion defined by the following equation

$$\Lambda_S = \max \lambda_S(\Gamma x, \Gamma y).$$

18. The random function generating method of claim 16 or 17, wherein:

said step (c-5) includes a step of: when no candidate function remains undiscarded, easing the candidate function selecting condition by changing said fifth reference by a fifth predetermined width, and executing again the evaluation and selecting process; and

said step (c-6) includes a step of: when no candidate function remains undiscarded, easing the candidate function selecting condition by changing said sixth reference by a sixth predetermined width, and executing again the evaluation and selecting process.

a 19. The random function generating method of claim 13, ~~14, or 15,~~ 14 wherein said candidate functions are each a composite function composed of at least one function resistant to said differential cryptanalysis and said linear cryptanalysis and at least one function of an algebraic structure different from that of said at least one function.

20. A recording medium having recorded thereon a random function generating method as a computer program, said program comprising the

steps of:

(a) setting various values as each parameter for candidate functions and calculating output values corresponding to various input values;

(b) storing the results of said calculation in storage means; and

(c) evaluating the resistance of each of said candidate functions to a cryptanalysis based on values stored in said storage means, and selectively outputting candidate function highly resistant to said cryptanalysis; and

wherein said step (c) comprising at lease one of:

(c-1) a higher-order cryptanalysis resistance evaluating step of: calculating the minimum value of the degree of a Boolean polynomial for input bits of each of said candidate functions by which its output bits are expressed; evaluating the resistance of said each candidate function to higher order cryptanalysis based on the result of said calculation; and leaving those of said candidate functions whose resistance is higher than a predetermined first reference and discarding the others;

(c-2) a differential-linear cryptanalysis resistance evaluating step of: calculating, for every set of input difference Δx and output mask value Γy of each candidate function S(x), the number of inputs x for which the inner product of $(S(x)+S(x\Delta x))$ and said output mask value Γy is 1; evaluating the resistance of said function to differential-linear cryptanalysis based on the result of said calculation; and leaving those of said candidate functions whose resistance is higher than a predetermined second reference and discarding the others;

(c-3) a partitioning-cryptanalysis resistance evaluating step of: dividing all inputs of each candidate function and the corresponding outputs into input subsets and output subsets; calculating an imbalance of the relationship between the subset of an input and the subset of the

corresponding output with respect to their average corresponding relationship; evaluating the resistance of said each candidate function to said partitioning cryptanalysis based on the result of said calculation; and leaving those of said candidate functions whose resistance is higher than a predetermined third reference and discarding the others; and

(c-4) an interpolation-cryptanalysis resistance evaluating step of: when fixing a key y and letting x denote the input of said each candidate, expressing an output y by y = $f_k(x)$ using a polynomial over Galois field which is composed of elements equal to a prime p or a power of said prime p; calculating the number of terms of said polynomial; evaluating the resistance of said function to interpolation cryptanalysis; and leaving those of said candidate functions whose resistance is higher than a predetermined fourth reference and discarding the others.

21. The recording medium of claim 20, wherein:

said differential-linear-cryptanalysis resistance evaluating step (c-2) includes a step of: letting the output mask value be represented by Γy, calculating the following equation for every set of said input difference Δx except 0 and said output mask value Γy except 0

$$\xi_S(\Delta x, \Gamma y) = \left| 2 \times \#\{x \in GF(2)^n | (S(x) + S(x + \Delta x)) \bullet \Gamma y = 1\} - 2^n \right|;$$

calculating the maximum value Ξ among the calculation results; and evaluating the resistance of said candidate function to said differential-linear cryptanalysis based on said value Ξ; and

said partitioning0cryptanalysis resistance evaluating step (3) includes a step of dividing an input set F and an output set G of said function into u input subsets $\{F_0, F_1, \ldots, {}_{Fu-1}\}$ and v output subsets $\{G_0, G_1, \ldots, G_{v-1}\}$; for each partition-pair (F_i, G_i) (i = 0, ..., u-1; j = 0, 1, ..., v-1), calculating the

maximum one of probabilities that all outputs y corresponding to all inputs x of the input subset F_i belong to the respective output subsets G_j ($j = 0, \ldots, v-1$); calculating a measure $I_S(F, G)$ of an average imbalance of a partition-pair (F, G) based on all maximum values calculated for all partition pairs; and evaluating the resistance of said candidate function to said partitioning cryptanalysis based on said measure.

22. The recording medium of claim 20 or 21, wherein:

said step (c-1) includes a step of: when no candidate function remains undiscarded, easing the candidate function selecting condition by changing said first reference by a first predetermined width, and executing again the evaluation and selecting process;

said step (c-2) includes a step of: when no candidate function remains undiscarded, easing the candidate function selecting condition by changing said second reference by a second predetermined width, and executing again the evaluation and selecting process;

said step (c-3) includes a step of: when no candidate function remains undiscarded, easing the candidate function selecting condition by changing said third reference by a third predetermined width, and executing again the evaluation and selecting process; and

said step (c-4) includes a step of: when no candidate function remains undiscarded, easing the candidate function selecting condition by changing said fourth reference by a fourth predetermined width, and executing again the evaluation and selecting process.

23. The recording medium of claim 20 or 21, wherein said program includesat least one of:

(c-5) a differential-cryptanalysis resistance evaluating step of: calculating, for each candidate function S(x), the number of inputs x that

satisfy S(x)+S(x+S(x+Δx)=Δy for every set (Δx, Δy) except Δx; evaluating the resistance of said each candidate function to differential cryptanalysis based on the result of said calculation; and leaving those of said candidate functions whose resistance is higher than a predetermined fifth reference and discarding the others; and

(c-6) a linear-cryptanalysis resistance evaluating step of: calculating, for each candidate function, the number of inputs x for which the inner product of the input x and its mask value Γx is equal to the inner product of a function output value S(x) and its mask value Γy; evaluating the resistance of said each candidate function to linear cryptanalysis based on the result of said calculation; and leaving those of said candidate functions whose resistance is higher than a predetermined sixth reference and discarding the others.

24. The recording medium of claim 23, wherein:

said differential-cryptanalysis resistance evaluating step (c-5) includes a step of: calculating the following equation

$$\delta_S(\Delta x, \Delta y) = \#\{x \in GF(2)^n \mid S(x) + S(x + \Delta x) = \Delta y\}$$

for every set of difference values (Δx, Δy) except Γy=0; and evaluating the resistance of said each candidate function to said differential cryptanalysis based on a criterion defined by the following equation

$\Delta_S = \max \delta_S(\Delta x, \Delta y)$; and

said linear-cryptanalysis resistance evaluating step (c-6) includes a step of: calculating the following equation

$$\lambda_S(\Gamma x, \Gamma y) = \left| 2 \times \# \{x \in (2)^n \mid x \bullet \Gamma x = S(x) \bullet \Gamma y\} - 2^n \right|$$

for every set of mask values (Γx, Γy); and evaluating the resistance of said each candidate function to said linear cryptanalysis based on a criterion

defined by the following equation

$\Lambda_S = \max \lambda_S(\Gamma x, \Gamma y)$.

25. The recording medium of claim 23 or 24, wherein:

said step (c-5) includes a step of: when no candidate function remains undiscarded, easing the candidate function selecting condition by changing said fifth reference by a fifth predetermined width, and executing again the evaluation and selecting process; and

said step (c-6) includes a step of: when no candidate function remains undiscarded, easing the candidate function selecting condition by changing said sixth reference by a sixth predetermined width, and executing again the evaluation and selecting process.

26. The recording medium of claim 20, 21 ~~21, or 22~~, wherein said candidate functions are each a composite function composed of at least one function resistant to said differential cryptanalysis and said linear cryptanalysis and at least one function of an algebraic structure different from that of said at least one function.

27. A recording medium having recorded thereon as a program a method for evaluating the randomness of the input/output relationship of a function, said program comprising at least one of:

(a) a higher-order-differential cryptanalysis resistance evaluating step of: letting said function be represented by S(x), calculating the minimum value of the degree of a Boolean polynomial for input bits of said function S(x) by which its output bits are expressed; and evaluating the resistance of said function to higher order cryptanalysis based on the result of said calculation;

(b) a differential-linear cryptanalysis resistance evaluating step of: calculating, for every set of input difference Δx and output mask value Γy

of a function S(x) to be evaluated, the number of inputs x for which the inner product of (S(x)+S(x Δ x)) and said output mask value Γy is 1; and evaluating the resistance of said function to differential-linear cryptanalysis based on the result of said calculation;

(c) a partitioning-cryptanalysis resistance evaluating step of: dividing all inputs of a function to be evaluated and the corresponding outputs into input subsets and output subsets; calculating an imbalance of the relationship between the subset of an input and the subset of the corresponding output with respect to their average corresponding relationship; and evaluating the resistance of said function to partitioning cryptanalysis based on the result of said calculation; and

(d) an interpolation-cryptanalysis resistance evaluating step of: when fixing a key y and letting x denote the input of said each candidate, expressing an output y by y = f_k(x) using a polynomial over Galois field which is composed of elements equal to a prime p or a power of said prime p; calculating the number of terms of said polynomial; and evaluating the resistance of said function to interpolation cryptanalysis.

28. The recording medium of claim 27, wherein:

said differential-linear cryptanalysis resistance evaluating step (b) is a step of:, letting the input difference and output mask value of said function S(x) be representing by Δx and Γy, respectively, calculating the following equation for every set of said input difference Δx except 0 and said output mask value Γy except 0

$$\xi_S(\Delta x, \Gamma y) = \left| 2 \times \#\{x \in GF(2)^n \middle| (S(x) + S(x+\Delta x) \bullet \Gamma y = 1\} - 2^n \right|;$$

calculating the maximum value Ξ among the calculation results; and evaluating the resistance of said function to said differential-linear

cryptanalysis using said value Ξ; and

said partitioning-cryptanalysis resistance evaluating step (c) is a step of: dividing an input set F and an output set G of said function into u input subsets $\{F_0, F_1, \ldots, {}_{Fu-1}\}$ and v output subsets $\{G_0, G_1, \ldots, G_{v-1}\}$; for each partition-pair (F_i, G_i) $(i = 0, \ldots, u-1; j = 0, 1, \ldots, v-1)$, calculating the maximum one of probabilities that all outputs y corresponding to all inputs x of the input subset F_i belong to the respective output subsets G_j $(j = 0, \ldots, v-1)$; calculating a measure $I_S(F, G)$ of an average imbalance of a partition-pair (F, G) based on all maximum values calculated for all partition pairs; and evaluating the resistance of said function to said partitioning cryptanalysis based on said measure.

29. The recording medium of claim 27 or 28, said program further comprising at least one of:

(e) a differential-cryptanalysis resistance evaluating step of: letting the output difference value of said function S(x) be represented by Δx, calculating the number of inputs x that satisfy $S(x)+S(x+S(x+\Delta x)=\Delta y$ for every set $(\Delta x, \Delta y)$ except $\Delta x=0$; and evaluating the resistance of said function to differential cryptanalysis based on the result of said calculation; and

(f) a linear-cryptanalysis resistance evaluating means for calculating, for said function S(x), the number of inputs x for which the inner product of the input x and its mask value Γx is equal to the inner product of a function output value S(x) and its mask value Γy and evaluating the resistance of said function to linear cryptanalysis based on the result of said calculation.

30. The recording medium of claim 29, wherein, letting the number of bits of said input x be represented by n:

said differential-cryptanalysis resistance evaluating step (e) is a step

of: calculating the following equation

$$\delta_S(\Delta x,\Delta y)=\#\{x\in GF(2)^n \mid S(x)+S(x+\Delta x)=\Delta y\}$$

for every set of difference values (Δx, Δy) except Δx=0; and evaluating the resistance of said function to said differential cryptanalysis based on a criterion defined by the following equation

$\Delta_S = \max \delta_S(\Delta x,\Delta y)$; and

said linear-cryptanalysis resistance evaluating step (f) is a step of: letting the mask value of said input x be represented by Γx, calculating the following equation

$$\lambda_S(\Gamma x,\Gamma y)=\left|2\times\#\{x\in(2)^n \mid x\bullet\Gamma x = S(x)\bullet\Gamma y\}-2^n\right|$$

for every set of mask values (Γx, Γy) except Γy=0; and evaluating the resistance of said function to said linear cryptanalysis based on a criterion defined by the following equation

$\Lambda_S = \max \lambda_S(\Gamma x,\Gamma y)$.